



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,378	11/16/2001	Dorothy E. Denning	774070-8	7029

23879 7590 09/07/2005

BRIAN M BERLINER, ESQ  
O'MELVENY & MYERS, LLP  
400 SOUTH HOPE STREET  
LOS ANGELES, CA 90071-2899

EXAMINER

POLTORAK, PIOTR

ART UNIT PAPER NUMBER

2134

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

h

## Office Action Summary

Application No.

09/992,378

Applicant(s)

DENNING ET AL

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 17 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-6,8-32 and 34-50 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6,8-32 and 34-50 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. The Amendment, and remarks therein, received on 6/17/2005 have been entered and carefully considered.
2. The Amendment introduces a new limitation into the originally sole independent claims 1, 28 and 45 and amended dependent claims 2-5, 11-12, 14-15, 18-20, 29-30, 36, 40, 46-48. Claims 7 and 33 have been cancelled.

The newly introduced limitation has required a new search and consideration of the pending claims. The new search has resulted in newly discovered prior art. New grounds of rejection based on the newly discovered prior art follow below.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.
4. Claims 1-6, 8-32 and 34-50 have been examined.

### ***Claim Rejections - 35 USC § 112***

5. Claims 1, 28 and 45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.
6. Claim 1 recites steps included in a method for controlling access to digital information. The method discloses two steps that are completed in regard to a data

Art Unit: 2134

encrypting key: modifying the data encrypting key using location data and encrypting the location-modified data encrypting key using a key encrypting key.

However, previously disclosed claims as well as applicant's specification disclose only encrypting the data encrypting key using a key encrypting key and location data.

7. Claims 28 and 45 are subject to the same rejection and claims 2-6, 8-27, 29-32, 34-44 and 46-50 are rejected by virtue of their dependencies.

***Claim Rejections - 35 USC § 112***

8. Claims 5-6, 14-15 and 46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
9. Applicant failed to address the second paragraph of the 35 U.S.C. 112 rejection directed towards claim 6 as stated in the previous Office Action. Claim 6 remains rejected and the examiner continues to treat the claim as best understood.
10. As per claims 14-15 and 46 it is unclear whether the phrase "precluding decryption of said encrypted digital information" is intended to mean that one is not able to retrieve the encrypted digital information or whether the process of decryption is disabled. Since applicant follows "precluding decryption" with "said encrypted digital information" for purposes of further examination the phrase is treated as the retrieval of the original digital information is precluded.

11. "Said location identify data" in claim 5 is not understood and lacks antecedent basis.

For purposes of further examination the phrase is treated as "said location identity data".

***Claim Rejections - 35 USC § 103***

12. Claims 1, 8, 11, 13-16, 28, 34, 37-38, 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Menezes (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237)* in view of *Laurance et al. (U.S. Patent No. 4860352)*.

13. As per claims 1 and 28 *Menezes* teaches encrypting digital information using a data encrypting key which generates the encrypted digital information (*Menezes, pg. 16 Fig. 1.7*), which also reads on encrypting said digital information using a data encrypting key, and encrypting the data encrypting key using a key encrypting key (*Menezes, "Point-to-point key update using symmetric encryption", in particular "key transport with one pass" section, pg. 497-498*), which reads producing an encrypted location-modified data encrypting key produced by encrypting the data encrypting key using a key encrypting key.

14. *Menezes* does not explicitly teach modifying the data encrypting key using location identity data that defines at least a specific geographic location.

15. *Laurance et al.* teach modifying (encryption) using a specific geographical location (*Abstract and col. 23 lines 1-10*) in order to prevent reading of the encrypted message by other receivers.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key. One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent unauthorized access to the data.

16. As per claims 8, 30 and 34 *Laurance et al.* teach location identity that defines the location of the intended receiver (*col. 23 lines 2-3*).

17. As per claims 11 and 45 it is implicit that the recipient would conduct the steps in reversal in order to retrieve plaintext.

18. As per claims 13 and 37 Official Notice is taken that it is old and well-known practice to use secure means to distribute digital information such as secret keys between two parties given the benefit of restricting access to digital information such as secret keys (e.g. session keys) in order to increase key distribution security.

19. The limitations of claims 14-15 and 46 are implicit; using incorrect keys would not decrypt encrypted data. Also, using session keys and/or preventing decryption at other than a designated location would not make sense if two entities were directly connected without any intermediate nodes (*distributors*) e.g. routers in between them.

20. As per claims 16 and 38 Official Notice is taken that it is old and well-known practice to engage at least one distributor (*intermediate node*) when routing (encrypted and non-encrypted) digital information. One of ordinary skill in the art at the time of

applicant's invention would have been motivated to employ at least one distributor in order to be able to route information to various remote recipients.

21. Claims 2-6, 9-10, 12, 18-19, 29-31, 35-36, 39, 47 are rejected under 35 U.S.C.

103(a) as being unpatentable over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Laurance et al.* (*U.S. Patent No. 4860352*) and in further view of *Murphy* (*U.S. Patent No. 6317500*).

22. As per claims 2-3, 9-10, 29 and 36 *Menezes* in view of *Laurance et al.* teach location identity as discussed above.

23. *Menezes* in view of *Laurance et al.* do not teach that the location identity data further comprise at least a location value and a proximity value of the specific geographic location of the recipient and that a GPS receiver is used in recovering the location.

24. *Murphy* teaches the location identity attribute comprising at least a location value (*location coordinates  $x(i)$ ,  $y(i)$ ,  $z(i)$* ), and a proximity value (*the diameter  $d(i)$  of the region  $R$  ( $L(i)$ ,  $d(i)$ )*) of the specific geographic location, the location value corresponding to a location of an intended receiver of the digital information, communicating the encrypted digital information to a receiver of the digital information disposed at the specific geographic location, and a location identifying step comprising recovering the location from a GPS receiver (*Murphy, col. 7 line 55 - col. 8 line 28 and col. 6 lines 46-65*).

25. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include at least a location value and a proximity value, and use a GPS to

recover the location as taught by *Murphy*. One of ordinary skill in the art would have been motivated to perform such a modification in order to allow data retrieval to only a certain region.

26. As per claims 4, 6 and 31-32, GPS location inherently describes the longitude and latitude of a location and the proximity value inherently corresponds to a zone that encompasses the location.

27. As per claim 5 location identity data as taught by *Menezes* in view of *Laurance et al.* is to enable the decryption process at a specific location. However, it is well known in the art that certain signals may not be intended for just the specific location (e.g. broadcast) and also that some situations may need portability (e.g. travel with a laptop). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include ability for the location identity data to define a universal location that encompasses the entire earth within the location value. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide security whenever there is a need to lift the limit on the location at which the data can be received.

28. Claims 21-27, 41-44, 49-50 are rejected under 35 U.S.C. 103(a) as being obvious over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Laurance et al.* (*U.S. Patent No. 4860352*) and in further view of *Schneier* (*Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457*).



Art Unit: 2134

29. *Menezes* and *Laurance* teach the data encryption key as discussed above.

*Menezes* and *Laurance* do not explicitly teach generating the data encryption key using a pseudo-random number generator.

*Schneier* teach generating the data encryption key using a pseudo-random number generator (*Schneier*, pg. 173, *Random Keys* section). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to generate the data encryption key using a pseudo-random number generator as taught by *Schneier*.

One of ordinary skill in the art would have been motivated to perform such a modification in order to assure appropriate strength of the key (*Schneier*, pg. 170-173).

30. Claim 19 is rejected under 35 U.S.C. 103(a) as being obvious over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Laurance et al.* (U.S. Patent No. 4860352) and *Schneier* (*Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457*) and in further view of *Murphy* (U.S. Patent No. 6317500).

31. *Murphy* teach GPS and *Menezes* in view of *Laurance* and *Schneier* teach generating the data encrypting key using a pseudo-random number generator as discussed above.

32. Although none of the references explicitly teach that generating the encryption key comprises using GPS signals to partially seed the pseudo-random number generator the choice of utilizing GPS signals would have been obvious to one of ordinary skill

Art Unit: 2134

in the art at the time of applicant's invention to provide the range of signals and constant changes in satellite positioning. One of ordinary skill in the art would have been motivated to utilize GPS signals to partially seed the pseudo-random number generator in order to take advantage of the large set of possible and constantly changing data that decrease predictability of the choice.

33. Claims 21-27 and 41-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Menezes* (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237) in view of *Laurance et al.* (U.S. Patent No. 4860352) and in further view of *Shibata et al.* (U.S. Patent No. 5586185).

34. As per claims 21, 41 and 49 *Menezes* in view of *Laurance et al.* teach storing the key encrypting key as discussed above.

35. *Menezes* in view of *Laurance et al.* do not explicitly teach a key table used for storing a plurality of keys including a key encrypting key.

36. *Shibata et al.* teach a key table for storing a plurality of keys (*Shibata et al. col. 1 line 55 – col. 2 line 23*).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a table to store a plurality of keys (including a key encrypting key) as taught by *Shibata et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to allow secure communication for multiple providers (*Shibata et al., col. 1 lines 7- 67*).

37. As per claims 22-25 and 50 *Shibata et al.* teach associating the plurality of keys with respective providers of the digital information, remote administering management comprising adding, changing or deleting any one of the plurality of keys in the key table (*Shibata et al.*, col. 1 line 55 – col. 2 line 23).

38. As per claims 26-27 *Menezes* teaches keys for signing data and validating signatures (*Menezes*, pg. 28). Furthermore, *Menezes* teaches that digital signature provides authentication, authorization, and non-repudiation.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include keys for signing data, to validate signatures and include a signature when adding, changing or deleting any one of the plurality of the secret keys in the key table. One of ordinary skill in the art would have been motivated to perform such a modification in order to establish authenticity of the keys (*authentication and non-repudiation*).

39. Claims 17, 20, 40 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Laurance et al.* (U.S. Patent No. 4860352) and *Inoue et al.* (U.S. Patent No. 6240514).

40. *Menezes* in view of *Laurance et al.* teach recovering the data encrypting key from the encrypted location-modified data encrypting key using a key decrypting key and a location value as discussed above and routing encrypted data to at least one distributor as discussed above.

41. *Menezes* in view of *Laurance et al.* do not teach decrypting and re-encrypting a location-modified data encrypting key.
42. *Inoue et al.* teaches encrypting digital information using a data encrypting key which generates the encrypted digital information, which reads on associating the encrypted data encrypting key with the encrypted digital information that could be accessed only at a specific location, encrypting the data encrypting key using a key encrypting key, decrypting the encrypted data encrypting key, and re-encrypting the data encrypting key using a different encrypting key (*Inoue et al.*, col. 4 line 49- col. 5 line 3).
43. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to decrypt and re-encrypt a location-modified data encrypting key as taught by *Laurance et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to increase data security along the path from a sender to a final destination.
44. Claims 17, 20, 40 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Laurance et al.* (U.S. Patent No. 4860352) and in further view of *Jones et al.* (U.S. Patent No. 6434699).
45. *Menezes* in view of *Laurance et al.* teach recovering the data encrypting key from the encrypted location-modified data encrypting key using a key decrypting key and

Art Unit: 2134

a location value as discussed above and routing encrypted data to at least one distributor as discussed above.

46. *Menezes* in view of *Laurance et al.* do not teach decrypting and re-encrypting location-modified data encrypting key.

47. *Jones et al.* teach a link encryption wherein data is encrypted and re-encrypted along the path from a sender to a final destination (*col. 5 lines 49-55*).

48. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to decrypt and re-encrypt a location-modified data encrypting key as taught by *Jones et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to increase data security along the path from a sender to a final destination.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of


Art Unit: 2134

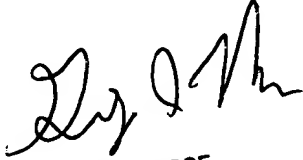
the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Signature  
  
9/2/05  
Date

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100